FedRAMP

Federal Risk Authorization Management Program

FedRAMP Forward

2 Year Priorities

December 17, 2014

FedRAMP

Federal Risk Authorization Management Program

In December 2010, the White House published the "25 Point Implementation Plan to Reform Federal IT."[1] A key component of that plan, the "Cloud First" policy, marked the U.S. Government's fundamental shift to defaulting to cloud computing solutions when secure, reliable, cost-effective options existed. One of the biggest obstacles to accelerating cloud adoption was ensuring that cloud computing solutions were secure. The Administration established the Federal Risk and Authorization Management Program (FedRAMP) in December 2011 to address security in cloud computing environments, in a manner that would build trust in authorizations and drive re-use to more quickly and cost-effectively achieve government-wide cloud adoption.[2]

FedRAMP launched operations in June of 2012 when its governing body, the Joint Authorization Board (JAB)[3], formally established the FedRAMP baseline security authorization requirements following an extensive government-wide vetting and public comment period. The Administration charged GSA with standing-up the FedRAMP Program Management Office (PMO) to create a framework by which agencies could use the baseline security authorization requirements to assess, authorize and continuously monitor cloud computing solutions. The framework uses the NIST 800 series Special Publications to ensure that all authorizations are fully compliant with the Federal Information Security Management Act (FISMA).

The FedRAMP baseline security requirements and unified framework for authorizing cloud environments allow Federal agencies to safely and securely use the cloud, and enables re-use of these authorizations under FISMA. With the average FISMA security authorization costing the U.S. Government upwards of $250,000, a framework by which agencies can re-use these authorizations is critical. FedRAMP's "do once, use many times" framework creates a multiplier effect of cost savings for agencies using the same cloud environments.

All Federal agencies must meet the FedRAMP requirements when using any cloud services. During the first two and a half years of operations, FedRAMP has made a significant impact on cybersecurity:

- 27 cloud service providers (CSPs) are FedRAMP compliant,
- 160+ FISMA implementations are covered by these authorizations,
- A Third Party Assessment Organization (3PAO) accreditation program for independent auditors to complete FedRAMP security assessments has been established,

[1] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/25-point-implementation-plan-to-reform-federal-it.pdf

[2] https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf

[3] The Joint Authorization Board (JAB) is comprised of the Chief Information Officer's (CIOs) from the Department of Defense (DOD), Department of Homeland Security (DHS) and the General Services Administration (GSA).

- 31 3PAOs are accredited; two thirds of which are small businesses,
- A conservative estimate of $40 million in cost savings has been achieved with less than $13 million invested in FedRAMP creation, and
- Creation of a cybersecurity framework industry and other nations are using to model their own cyber efforts.

FedRAMP's success can be attributed to its core principles of transparency, consensus building, and stakeholder trust and buy-in. FedRAMP developed "FedRAMP Forward: Two Year Priorities" to share key objectives, continue to expand and enhance the program effectively, and address key program issues critical to continued success.

FedRAMP Forward prioritizes three key areas of focus. First, increased stakeholder engagement is needed to more fully realize the benefits of FedRAMP across the government. Second, improving efficiencies will allow the FedRAMP process to happen faster and with fewer hurdles. And third, continuing to adapt is critical to staying aligned with the evolving cybersecurity landscape. This plan sets out the objectives and initiatives FedRAMP will pursue over the next two years to address these key issues.

INCREASE STAKEHOLDER ENGAGEMENT

FedRAMP and its application to cloud environments is complex and involves a broad array of stakeholders: Federal agencies, 3PAOs, and CSPs. One of the keys to success through FedRAMP is ensuring that stakeholders fully understand the requirements and are actively engaged through the process, from initiation, to authorization, and continuous monitoring.

There are more than 50 CSPs actively engaged in the FedRAMP process, 31 accredited 3PAOs, and nearly every Federal agency is participating in FedRAMP. But these numbers don't reflect the true marketplace of cloud systems in the Federal government. In order to reach the full breadth of cloud providers working with the Federal government as well as encourage new and innovative services to be available for use, stakeholder engagement with FedRAMP needs to increase.

INCREASE NUMBER OF AGENCIES IMPLEMENTING FEDRAMP

In many departments and agencies, FedRAMP implementation is limited to specific programs and the cloud services they are using, rather than being done in an enterprise-wide manner across departments and agencies. FedRAMP implementation will be expanded by:

- Establish accurate FedRAMP metrics: The FedRAMP PMO will work to better analyze the true breadth of use of FedRAMP across the government – not just through PortfolioStat analysis – but through the identification of usage across small and micro agencies, congressional and judicial branch entities, and state and local governments.
- Creating practical implementation guidance: Guidance will address all use cases of implementations – including beginning an assessment, re-using an existing assessment, implementing agency responsibilities, transitioning legacy applications in to a cloud infrastructure, and more.
- Additional support for FedRAMP: It takes people to implement FedRAMP. Many agencies rely on contract resources to assist in their efforts to implement FedRAMP. Identification of procurement options for agencies to find the specialized expertise needed will be important for agency implementation efforts.

INCREASE CROSS-AGENCY COLLABORATION

At the heart of FedRAMP is the principle of "do once, use many times." The more the Federal government works together to implement FedRAMP, the more cost savings and efficiencies agencies can realize. The PMO will assist agencies collaborating under FedRAMP by:

- Developing a multi-agency framework: Many CSPs have footprints and established use across multiple agencies. How to effectively and efficiently manage these environments in a collaborative manner needs to be further clarified to establish defined roles and responsibilities to maximize re-use and reduce duplication.
- Launching working groups: FedRAMP will Formally launch FedRAMP working groups which will give agencies a forum to collaborate as they work through FedRAMP assessments, authorizations and continuous monitoring.
- Ensuring JAB P-ATOs cover government-wide use: The JAB's mission is to support CSPs that support the broadest range of government-wide use. The working groups and multi-agency framework will allow the JAB to transition systems they have provisionally authorized to agencies for continuous monitoring for those services that do not reach broad government-wide use.

INCREASE UNDERSTANDING OF FEDRAMP

A clear understanding of FedRAMP and all of its requirements is imperative to any implementation efforts by stakeholders. After two and a half years there have been many lessons learned and a better understanding of the nuances of meeting FedRAMP requirements. To make sure that stakeholders not only understand FedRAMP but benefit from the lessons learned, the PMO will:

- Re-launch FedRAMP.gov: Information is useless if it cannot be found. The FedRAMP website will be re-launched in a more user friendly format and re-organized so users can more easily and quickly find the information they need.
- Launch Formal Training: FedRAMP is a complex framework with many operational processes across a myriad of stakeholders and responsibilities. All stakeholders need to understand their responsibilities under this framework. A formal training program will help stakeholders gain deeper knowledge and understanding of FedRAMP. The training program will launch with a focus on the key FedRAMP requirements for assessments and authorizations, and will grow to include specific modules targeted to defined stakeholder groups like program managers and procurement officials.
- Continued Updates to Reference and Guidance Documents: As more agencies move to the cloud and more systems are in use across the Federal government, it is important to share lessons learned. FedRAMP initiated this with the Guide to Understanding FedRAMP. This document will be expanded and continually updated to include those lessons learned over time.

IMPROVE EFFICIENCIES

The FedRAMP Security Assessment Framework (SAF) is complex with multiple stakeholders and many dependencies. The process can take anywhere from four months to more than a year to complete. Since June 2012, FedRAMP has developed benchmarks to better understand the level of effort it takes to meet the FedRAMP requirements. These benchmarks have identified key areas in which efficiencies could be realized to reduce the overall time and level of effort required by stakeholders.

Improving efficiency will be critical to the success of many CSPs, 3PAOs and agencies in meeting the FedRAMP requirements and will help reduce the time and cost for the security authorization process, and will help open up the Federal market to smaller and more niche service providers giving the Federal government a greater market of IT providers from which to choose.

ENHANCE CONSISTENCY AND QUALITY OF 3PAO ASSESSMENTS AND DELIVERABLES

FedRAMP is the only program that accredits independent assessors for Federal cybersecurity standards through the 3PAO accreditation program. 3PAOs provide the government with the independent verification and validation of a CSP's security implementations and identify any associated risks. The government bases its decision to authorize a service provider on a 3PAOs assessment and accompanying report. Through the 3PAO accreditation program, the PMO will:

- Update 3PAO accreditation requirements: The current 3PAO requirements have broad applicability through ISO 17020 and a FedRAMP knowledge test. The PMO will incorporate 3PAO Guidelines for specific FedRAMP applications to 3PAO policies and processes in to the official 3PAO requirements.
- Training program for 3PAOs: Training programs for 3PAOs will be developed specifically to address the nuances of security assessments in a cloud environment as well as quality control in the delivery of documentation to the government. This training will be mandatory for 3PAO assessors to complete and be a part of FedRAMP assessments.

ESTABLISH A FLEXIBLE FRAMEWORK FOR DATA AND WORKFLOW MANAGEMENT

Automation is already a part of a cloud service providers offering through things like internal management of a cloud service, customer self service provisioning, and elasticity of services consumed. There are existing tools that agencies and CSPs use to automate parts of the FedRAMP process, however not all of them meet FedRAMP documentation requirements and there is not a consistent set of requirements for how systems should incorporate automated data feeds from vendors to analyze. In order to realize automation in these areas the PMO will:

- Identify existing automation capabilities: Since there are already players in this space across not only government but industry, FedRAMP will identify and work with these existing service providers to better understand their tools and the scope of their capabilities.
- Develop FedRAMP specific automation requirements: FedRAMP requires specific formatting and templates in order to maximize re-use. As such, the development of FedRAMP specific automation requirements will help stakeholders apply automation in a way that can fully meet FedRAMP. These requirements will be created through an initial industry day with identified service providers and subsequent public comment periods.

RE-USE INDUSTRY STANDARDS

FedRAMP is not the only cybersecurity compliance standard. There are other examples of cybersecurity standards cloud providers might be required to meet – ISO, HIPAA, CIJIS, CSA STARS, SOC II – to name a few. Cloud providers that meet more than one of these compliance standards carry a heavy burden to meet all of these compliance frameworks. Many times CSPs are not able to re-use the evidence for compliance efforts from one framework to another. The goal of all cybersecurity compliance efforts is to demonstrate that an environment is secure enough to protect data according to various standards. In order to help CSPs and 3PAOs realize efficiencies in FedRAMP assessments and authorization through re-use of evidence across various compliance frameworks, the FedRAMP PMO will:

- Publish re-use requirements: Re-use of evidence will require a close attention to scoping and ensuring the evidence being re-used equally applies to two or more industry standards. The requirements must be clear as to what must be met in order to re-use evidence from one framework to another.
- Map re-use standards to industry requirements: Once the re-use requirements are complete, they will need to be applied to an industry standard for practical application and use. As these mappings are created, they will be piloted with CSPs and authorizing officials to ensure accuracy and develop lessons learned. These pilots will help formalize industry mappings and guide future efforts.

CONTINUE TO ADAPT

While there are seemingly strict confines around which FedRAMP was built, the key to FedRAMP's success is the adaptability of FISMA, NIST standards, and DHS guidance. In order for FedRAMP to continue its growth, it is recognized that the cybersecurity landscape evolves constantly – practically on a minute to minute basis – and the adaptability must also apply to FedRAMP as it continues to apply FISMA, NIST standards, and DHS guidance.

As the Federal government matures in its application of cybersecurity standards, there are opportunities for FedRAMP to help coordinate efforts among Federal agencies using CSPs. Adapting to meet the evolving cloud offerings and introduction of new services, the levels of data the government is placing in cloud environments, and placing a higher focus on overall risk management instead of compliance will keep FedRAMP ahead of the curve and ensure all stakeholder needs are being met.

EVOLVE CONTINUOUS MONITORING

Part of meeting the FedRAMP requirements includes adherence to the "FedRAMP Continuous Monitoring Strategy and Guide." This guide has three key areas: periodic reporting, change management, and incident response. Many of the requirements within the "FedRAMP Continuous Monitoring Strategy and Guide" are based on compliance activities. In order to have more effective continuous monitoring, risk management needs to be more fully incorporated. The FedRAMP PMO will evolve the continuous monitoring approach by:

- Updating continuous monitoring requirements: Through dialogue with service providers and Federal agencies, and key stakeholders like NIST and DHS, FedRAMP will update the continuous monitoring requirements to have a key focus on risk management through more real time views of CSP environments and establishing key indicators for reviewing CSP risks.
- Establish continuous monitoring reporting requirements: In order to effectively monitor agencies use of multiple environments across various CSPs, reporting of continuous monitoring needs to be done consistently. FedRAMP will create and refine reporting requirements so agencies will be able to re-use CSP continuous monitoring deliverables consistently across agencies.
- Correlate continuous monitoring activities across authorizations: As CSPs meet the continuous monitoring reporting requirements, correlating the data across all authorizations will give the Federal government a greater ability to understand risk as it relates across all applicable environments. FedRAMP will enable agencies to have insight to continuous monitoring data on all of the systems they use.

ESTABLISH ADDITIONAL BASELINES

FedRAMP launched with a baseline for low and moderate impact systems, which covers approximately 80% of Federal information systems. Over the last two and a half years, agencies have been rapidly moving to the cloud and showing a strong desire to move more and more mission critical services to the cloud, including some with higher sensitivity levels of data. To ensure that FedRAMP requirements and baselines meet these evolving stakeholder needs, the FedRAMP PMO will:

- Develop a high baseline: Almost since inception, all of the FedRAMP stakeholders have asked when a high baseline would be developed. The FedRAMP PMO will work with the JAB to develop a high impact baseline, and will coordinate the vetting process through the CIO Council, ISIMC, and multiple rounds of public comment.
- Identify additional baseline needs: FedRAMP will also continue to assess the need for additional baselines and develop those as necessary. Possibilities include systems that meet the requirements for high availability but only need moderate protections for confidentiality and integrity.

ENHANCE INTERGRATION WITH CYBER INITIATIVES AND CONTRIBUTE TO POLICY REFORM

Technology serves as the intersection for many Government-wide initiatives – and this provides agencies with a challenge to ensure they meet a multitude of requirements when using a single solution. Requirements such as the Trusted Internet Connection (TIC), Homeland Security Protocol Directive-12 (HSPD-12), Internet Protocol version 6 (IPV6), and Continuous Diagnostic and Mitigation (CDM) have critical requirements overlapping with some of the FedRAMP requirements. In order to address this challenge, the FedRAMP PMO will:

- Develop FedRAMP assessment overlays: Agencies, CSPs, and 3PAOs should be able to demonstrate compliance with multiple agency initiatives when undergoing any compliance activity. FedRAMP will create overlays to the FedRAMP Security Assessment Framework that will allow for assessments to demonstrate compliance with FedRAMP but also other initiatives like HSPD-12, IPv6, TIC, CDM, etc.
- Active engagement with broader cybersecurity community: FedRAMP will continue to work with our counterparts across the government at NIST, DHS, and OMB and through government councils like the CIOC and ISIMC to ensure the program's work continues to align with other IT initiatives and contribute to a more cohesive cybersecurity framework across government.

FedRAMP Forward: 2 Year Plan

As FedRAMP looks towards the next two years, FedRAMP Forward's goals are to continue the success of the program through the PMO engaging more directly with stakeholders to improve understanding of FedRAMP to ensure benefits of the program are fully realized. The PMO will also focus on finding key areas of efficiencies to make the FedRAMP process faster and to optimize utilization of stakeholder resources. Finally, FedRAMP will continue to evolve by addressing the changing needs of stakeholders and ensuring the program meets the ever evolving cybersecurity landscape.

The goals and key issues discussed have been translated in to a roadmap with deliverables roughly every six months. The PMO will continue to provide updates on progress on this roadmap and will evaluate the overall progress and validity of each initiative. FedRAMP will continue its foundation of consensus building and stakeholder buy in by keeping stakeholders actively engaged and informed about progress over the next two years as FedRAMP Forward is fully implemented.

APPENDIX A: OUTCOMES AND TIMELINES

OBJECTIVE	INITIATIVES AND OUTCOMES
6 Month Initiatives	
Increase number of agencies implementing FedRAMP	Baseline FedRAMP use across Federal government with various data points including PortfolioStat and FISMA reporting.
	Provide practical implementation guidance for agency ATOs for initiating assessments and authorizations, re-use of ATOs, and implementing solutions within an ATO cloud service.
Increase cross-agency collaboration	Publish draft multi-agency authorization methodology following FedRAMP Security Assessment Framework (SAF).
Increase understanding of FedRAMP	Develop and launch online FedRAMP training program.
	Re-launch FedRAMP.gov to improve user experience and usability.
	Publish agency procurement guidance (in collaboration with OMB / OFPP).
Enhance consistency and quality of 3PAO assessments and deliverables	Publish guidelines for 3PAOs to address inconsistencies for security assessment activities, artifacts and methodologies.
Establish a flexible framework for data and workflow management	Identify existing workflow tools, control automation, and document automation capabilities.
Re-use industry Standards	Publish draft requirements for re-use of external industry compliance evidence for assessment, authorization and continuous monitoring
Evolve Continuous Monitoring	Publish roadmap for evolution of continuous monitoring to include ongoing authorizations, near real time risk analysis, and greater emphasis on risk management.
	Publish guidelines with key indicators for authorizing officials to effectively perform risk analysis and more readily identify and respond to changes in risk posture of systems with existing authorizations.
Establish additional baselines	Publish draft high baseline for public comment.
Enhance integration with cyber initiatives and contribute to policy reform initiatives	Develop framework for FedRAMP assessment overlay for compliance with relevant IT policies (e.g. TIC, IPv6).
	Publish draft initial FedRAMP assessment overlay with 1 to 2 IT policies.

OBJECTIVE	INITIATIVES AND OUTCOMES
12 Month Initiatives	
Increase number of agencies implementing FedRAMP	Normalize agency reported data and enhance guidance on agency reporting of FedRAMP and cloud statistics through PortfolioStat.
	Document agency success stories for FedRAMP, establishing a best practice reference guide.
Increase cross-agency collaboration	Identify and launch working groups for multi-agency authorizations
	Publish draft multi-agency continuous monitoring methodology following FedRAMP SAF.
Increase understanding of FedRAMP	Develop FedRAMP training module for agency procurement officials.
Enhance consistency and quality of 3PAO assessments and deliverables	Develop FedRAMP 3PAO training module in concert with FedRAMP Accreditation Board.
	Update 3PAO requirements to ensure consistency for security assessment activities, artifacts and methodologies.
Establish a flexible framework for data and workflow management	Conduct Industry Day on tools and processes for automation of CSP documentation and assessment and continuous monitoring evidence.
Re-use industry standards	Identify and map one external industry compliance framework for re-use of evidence for assessment, authorization and continuous monitoring.
Evolve continuous monitoring approach	Publish guidelines and requirements for automating and correlating continuous monitoring data across agency and JAB authorized systems.
Establish additional baselines	Finalize high watermark baseline.
Enhance integration with cyber initiatives and contribute to policy reform initiatives	Conduct concurrent assessments of FedRAMP and additional IT policies.
18 Month Initiatives	
Increase number of agencies implementing FedRAMP	Identify procurement options for agencies to obtain FedRAMP implementation support
	Publish report documenting current status of FedRAMP metrics and statistics

OBJECTIVE	INITIATIVES AND OUTCOMES
Increase understanding of FedRAMP	Develop targeted FedRAMP training module for agency program managers.
Establish a flexible framework for data and workflow management	Publish draft requirements for automation of FedRAMP documentation.
Re-use industry standards	Complete pilot assessment of one CSP re-using evidence from external compliance framework.
Evolve continuous monitoring approach	Automate and correlate of continuous monitoring data across 2 agency and 2 JAB authorizations.
Establish additional baselines	Identify need for additional agency baseline requirements.
Enhance integration with cyber initiatives and contribute to policy reform initiatives	Finalize FedRAMP assessment overlay framework.
	Publish formal guidance methodology for assessment overlays IT mandates.
24 Month Initiatives	
Increase cross-agency collaboration	Transition of continuous monitoring from JAB to multi-agency model for JAB P-ATOs that do not reach or achieve government-wide use.
Increase understanding of FedRAMP	Continued updates to reference and guidance documents.
Establish a flexible framework for data and workflow management	Finalize automation requirements for FedRAMP documentation.
Re-use industry standards	Publish additional mappings of external industry compliance frameworks for evidence re-use.
Evolve continuous monitoring approach	Automate and correlate continuous monitoring and incident reporting data across all JAB and participating agency FedRAMP authorizations.
Establish additional baselines	Publish draft flexible baseline based on identified agency needs.
Enhance integration with cyber initiatives and contribute to policy reform initiatives	Develop two additional FedRAMP assessment overlays for compliance with additional IT initiatives.